

**AMENDMENTS TO THE SPECIFICATION**

Please amend the third full paragraph on page 10 as shown below:

--According to the present invention, before performing the substitution of step 34, state  $SR(S_i) + SR(R)$  is combined (block 42) with a value of same size  $(R1 + SR(R))$  corresponding to the application of the row shifting to random value R ( $SR(R)$ ) combined, byte by byte, by XOR with random value R1. In other words, the state is masked by a value of same size, each byte of which has the same random value.--